

**UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS**

DAVID HOUSE,

Plaintiff,

v.

**JANET NAPOLITANO, in her official capacity
as Secretary of the U.S. Department of
Homeland Security; ALAN BERSIN, in his
official capacity as Commissioner, U.S. Customs
and Border Protection; JOHN T. MORTON, in
his official capacity as Director, U.S.
Immigration and Customs Enforcement,**

Defendants.

Civil Action No. 11-10852-DJC

MEMORANDUM AND ORDER

CASPER, J.

March 28, 2012

I. Introduction

Plaintiff David House (“House”) has brought this action against Defendants Secretary of the United States Department of Homeland Security Janet Napolitano, Commissioner of United States Customs and Border Protection Alan Bersin, and Director of United States Immigration and Customs Enforcement John T. Morton (collectively, “the Defendants”), alleging that federal agents’ search of his electronic devices at the border and prolonged seizure of same for forty-nine days without reasonable suspicion (and retention and dissemination of the information contained therein) violated his rights under the Fourth Amendment to the United States Constitution (First Cause of Action) and the First Amendment to the Constitution (Second Cause of Action). House also alleges that the

Defendants' review, copying, retention and dissemination of the information contained on such devices violates his "right of associational privacy" under the First Amendment (Third Cause of Action). The Defendants have now moved to dismiss the complaint, or in the alternative, for summary judgment. For the reasons set forth below, the Defendants' motion to dismiss is DENIED.

II. Burden of Proof and Standard of Review

To survive a motion to dismiss, a complaint "must 'give the defendant fair notice of what the . . . claim is and the grounds upon which it rests,' and allege 'a plausible entitlement to relief.'" Decotiis v. Whittemore, 635 F.3d 22, 29 (1st Cir. 2011) (quoting Bell Atl. Corp. v. Twombly, 550 U.S. 544, 555, 559 (2007)). The Court accepts non-conclusory factual allegations in the complaint as true, Ocasio-Hernández v. Fortuño-Burset, 640 F.3d 1, 12 (1st Cir. 2011), and "draw[s] all reasonable inferences in favor of the plaintiff[]." Gargano v. Liberty Int'l Underwriters, Inc., 572 F.3d 45, 48 (1st Cir. 2009). "While a complaint attacked by a Rule 12(b)(6) motion to dismiss does not need detailed factual allegations, a plaintiff's obligation to provide the grounds of his entitlement to relief requires more than labels and conclusions, and a formulaic recitation of the elements of a cause of action will not do." Twombly, 550 U.S. at 545 (internal quotation marks and citations omitted). However, considering a motion to dismiss "is neither the time nor the place to resolve the factual disputes between the parties. Whether [the plaintiff] can prove what he has alleged is not the issue. At this stage of the proceeding we must take the complaint's factual allegations as true," as long as they paint "a plausible picture." Haley v. City of Boston, 657 F.3d 39, 52 (1st Cir. 2011).

A motion to dismiss may be converted to a motion for summary judgment "[a]t the discretion of the district court." Trans-Spec Truck Serv., Inc. v. Caterpillar, Inc., 524 F.3d 315, 321 (1st Cir. 2008) (citing Fed. R. Civ. P. 12(d)). Summary judgment is appropriate when "the pleadings,

depositions, answers to interrogatories, and admissions on file, together with the affidavits, if any, show that there is no genuine issue as to any material fact and that the moving party is entitled to judgment as a matter of law.” Am. Airlines, Inc. v. Cardoza-Rodriguez, 133 F.3d 111, 116 (1st Cir. 1998). Although the Defendants offer supplemental materials, including affidavits, the Court declines to treat the instant motion as one for summary judgment. To do so would be premature where the parties have yet to engage in discovery and the factual record is incomplete and where, as House contends, there appear to be material facts as to his claims that remain disputed at this juncture.

III. Factual Allegations

A. House’s Role in the Bradley Manning Support Network

The Court must accept as true the complaint’s factual allegations in considering the Defendants’ motion to dismiss. The complaint makes the following allegations. In June 2010, House and others organized political support for the defense of Bradley Manning, a United States serviceman deployed in Iraq who was arrested in May 2010 on suspicion of having disclosed restricted material to WikiLeaks. Compl. ¶¶ 9, 12. Manning’s arrest followed WikiLeaks’ publication of “Collateral Murder,” a video of U.S. forces killing Iraqi civilians during a 2007 air attack in Baghdad. Id. at ¶ 10. In July 2010, the United States Army formally charged Manning with accessing and disclosing classified information without authorization, including a “classified video of a military operation” and fifty State Department Cables. Id. at ¶ 9. The U.S. Army brought further charges against Manning in March 2011, including a charge that he knowingly gave intelligence to the enemy. Id. Following his arrest, Manning was moved to a military detention facility in Quantico, Virginia, where he was held until April 2011 in solitary confinement. Id. Both Manning’s alleged disclosure of government records and the suspected connection between Manning and WikiLeaks

were, at the time the complaint was filed, the subjects of ongoing criminal investigations. Id. at ¶ 11.

The Bradley Manning Support Network (“Support Network”), formed by House and others, is an unincorporated association of individuals and organizations. Id. at ¶ 12. The Support Network is an “international grassroots effort to help accused whistle blower Pfc. Bradley Manning.” Id. Its purpose is to harness the outrage of viewers of the “Collateral Murder” video into a coordinated effort in defense of Manning, coordinate international support for him, raise funds for his legal defense and provide him with support during his imprisonment. Id. The Support Network pursues these objectives through its website and internet presence, the organization of public events and private contact with individuals. Id. The Support Network is not affiliated with WikiLeaks. Id.

In addition to his role as a founding member of the Support Network, House developed the organization’s website. Id. at ¶ 12-13. House is a computer programmer and researcher by trade. Id. at ¶ 12. He currently serves on the Support Network’s Steering Committee and regularly communicates with others who are concerned about Manning’s treatment and prosecution. Id. at ¶ 13. House is also one of the Support Network’s primary fundraisers and has been responsible for meeting potential supporters and soliciting donations for Manning’s legal defense. Id.

In the complaint, House alleges he became the target of federal investigators following the creation of the Support Network. Id. at ¶ 14. He also claims he has been visited and questioned, both at his home and at his place of employment, by investigators for the Department of Defense, the Department of State, and the Federal Bureau of Investigation. Id. House further alleges that he has been the subject of ongoing surveillance. Id. He has been placed on a watch list, which has resulted in him being stopped for questioning and searched each time he enters the United States. Id. Since

September 2010, House contends he has been detained at the border on every occasion he has re-entered the United States after foreign travel and he has been questioned about his work with the Support Network or his political beliefs and activities. Id.

B. The November 3, 2010 Search and Seizure of House's Electronic Devices

On November 3, 2010, following a vacation in Mexico, House arrived at the Chicago O'Hare International Airport, where he was scheduled to catch a connecting flight to Boston. Id. at ¶ 15. At the time, House was carrying his laptop computer, a USB storage device, a video camera containing a memory storage device and a cellular phone. Id. Upon arrival, House passed through a passport control station, collected his baggage, and proceeded to customs, where a Customs and Border Protection ("CBP") officer advised him that his belongings would be searched. Id. The officer examined House's computer and noted that it was warm but did not attempt to open it. Id. House was then told he was free to leave. Id.

House proceeded to the terminal of his connecting flight to Boston. Id. at ¶ 16. After he entered the terminal and as he walked to his gate, two government agents stopped him. Id. The agents, identified by their nametags as Darin Louck and Marcial Santiago, stated that they were with the Department of Homeland Security ("DHS"). Id. Agents Louck and Santiago told House that he was being detained and would miss his connecting flight. Id. The agents told House that he would have to give them any electronic devices he was carrying, without explaining why or asking for House's consent. Id. at ¶ 17. House surrendered his computer, USB storage device, video camera and cellular phone. Id. House's computer and other electronic devices contained private and personal information and information concerning his work on behalf of the Support Network. Id. ¶ 28. Specifically, the devices contained House's personal e-mail communications covering a period

of several years, including messages sent to and from family members and friends and concerning employment related matters, records of his personal finances, computer programming works in progress, and passwords allowing access to his bank account, to his workplace computer and to secure communications websites. Id. at ¶ 29. The devices also contained information concerning the Support Network, including the complete Support Network mailing list, confidential communications between members of the Steering Committee about strategy and fund-raising activities, the identity of donors, lists of potential donors and their ability to contribute, and notes from meetings with donors including personal observations about those donors. Id. at ¶ 30.

The agents took the devices and directed House to wait. Id. at ¶ 17. When the agents returned a short time later, they were no longer in possession of the items they had taken. Id. The agents directed House to accompany them to an interrogation room, where he was initially asked a series of questions concerning the security of the computer. Id. at ¶ 18. He advised the agents that the computer's hard disk was not encrypted, but that the computer was password protected. Id. When asked, he declined to give them his password, explaining that providing the password would allow direct and unauthorized access to research on his employer's server. Id.

House alleges that Agents Louck and Santiago detained him for questioning for an extended period of time. Id. at ¶ 19. They questioned him about his association with Manning, his work for the Support Network, whether he had any connection to WikiLeaks, and whether he had been in contact with anyone from WikiLeaks during his trip to Mexico. Id. The agents did not ask House any questions related to border control, customs, trade, immigration or terrorism, and at no point did the agents suggest that House had engaged in any illegal activity or that his computer contained any illegal material. Id.

When House was allowed to leave, only his cell phone was returned to him. Id. at ¶ 20. The other items that had been taken—his computer, USB device and camera—were not returned. Id. The agents gave House a receipt listing the items that had been seized, indicating that “R. Hart, SAC CHI ICE” had taken custody of them, and the agents told him that his other items would be returned by FedEx within a week. Id.

On December 21, 2010, forty-eight days after the agents seized House’s electronic devices, they remained in government custody. Id. at ¶ 21. On that date, House, through counsel, sent a letter by facsimile to DHS, CBP and Immigration and Customs Enforcement (“ICE”) requesting that his electronic devices be returned to him immediately. Id. He also requested documentation of the chain of custody of any copies made of the information contained on his devices and documentation of their destruction. Id.

On December 22, 2010, House’s electronic devices were returned to him by mail from the “DHS CIS New York District Office.” Id. at ¶ 22. In a letter to House’s counsel dated December 30, 2010, general counsel for ICE noted that the devices had been returned but did not indicate whether any information derived from those devices had been copied, what agencies or individuals were given copies that were made, or whether any such copies had been destroyed. Id. at ¶ 23. The complaint alleges that the information “has been disclosed to and retained by other government agencies.” Id. at ¶ 27.

IV. Procedural History

On May 13, 2011, House filed the instant action against the Defendants. D. 1. The complaint alleges that the search and prolonged detention of House’s electronic devices and the Defendants’ continued retention and dissemination of the information they contained violate his rights under the

Fourth Amendment and the First Amendment to the United States Constitution, (First and Second Causes of Action, respectively, D. 1 at ¶¶ 36, 37), and that the interception and, specifically, the retention and dissemination of information in House’s computer and other electronic devices regarding the work, supporters and donors of the Support Network violates House’s “right of associational privacy” under the First Amendment. Third Cause of Action, D.1 at ¶ 38. House seeks both declaratory and injunctive relief. Prayer for Relief, D.1. On July 28, 2011, the Defendants moved to dismiss the complaint, or in the alternative, for summary judgment. D. 10. The Court held a hearing on the motion and took the matter under advisement.

V. Discussion

A. Fourth Amendment Challenge to the Initial Search and Seizure

1. Whether Some Level of Suspicion is Required for Searching a Traveler’s Electronic Devices at the Border

The Fourth Amendment guarantees “the right of the people to be secure in their persons . . . and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause” U.S. CONST. amend. IV. Although searches must be reasonable, “the Fourth Amendment’s balance of reasonableness is qualitatively different at the international border than in the interior.” United States v. Montoya de Hernandez, 473 U.S. 531, 538 (1985). The Fourth Amendment’s balancing test of interests leans heavily toward the government at the border.¹ See United States v. Ramsey, 431 U.S. 606, 619 (1977). This is so because “the United States, as sovereign, has the inherent authority to protect, and a paramount interest in

¹House does not contest that the November 3, 2010 search and seizure occurred at the border for the purposes of his constitutional claims. Pl. Opp. at 11 n. 5.

protecting, its territorial integrity.” United States v. Flores-Montano, 541 U.S. 149, 153 (2004); see also Carroll v. United States, 267 U.S. 132, 154 (1925) (concluding that “[t]ravelers may be so stopped in crossing an international boundary because of national self-protection reasonably requiring one entering the country to identify himself as entitled to come in, and his belongings as effects which may be lawfully brought in”). Because searches at the border are conducted pursuant to the government’s longstanding right to protect itself, the Supreme Court has stated that such searches are “reasonable simply by virtue of the fact that they occur at the border.” Flores-Montano, 541 U.S. at 152-53 (quoting Ramsey, 431 U.S. at 616). That is, “[r]outine searches of the persons and effects of entrants [into the United States] are not subject to any requirement of reasonable suspicion, probable cause, or warrant” Montoya de Hernandez, 473 U.S. at 538; see also United States v. Barrow, 448 F.3d 37, 41 (1st Cir. 2006).

The Supreme Court, however has recognized certain limitations to the border search power to conduct routine searches without some level of suspicion. First, customs officials may need some level of suspicion to conduct “highly intrusive searches” implicating the “dignity and privacy interests” of a person such as body cavity or strip searches. See Flores-Montano, 541 U.S. at 152 (holding that the removal, disassembly and reassembly of a vehicle’s fuel tank at the border did not require particularized suspicion). The Supreme Court has described strip, body cavity, or involuntary x-ray searches as “nonroutine border searches” but expressly declined to suggest “what level of suspicion, if any, is required” for these searches. Montoya de Hernandez, 473 U.S. at 541 n. 4. Second, other than “highly intrusive searches of the person,” Flores-Montano, 541 U.S. at 152, the Supreme Court has left open the question “whether, and under what circumstances, a border search might be deemed ‘unreasonable’ because of the particularly offensive manner in which it was carried out,” Id. at 155,

n. 2 (quoting Ramsey, 431 U.S. at 618 n.13), but has not defined the precise contours of a search carried out in such a manner. Third, the Supreme Court has suggested the possibility that “some searches of property are so destructive as to require” some level of suspicion. Flores-Montano, 541 U.S. at 155-56.

House’s Fourth Amendment challenge to the reasonableness of the border search of his laptop and other electronic devices is premised on the first two categories; House alleges that the search and seizure of his laptop computer and other electronic devices was highly intrusive given the personal nature and quality of information stored on these devices and because the search was conducted in a particularly offensive manner and such “non-routine” search would only have comported with the Fourth Amendment if the agents had some level of suspicion.²

Neither the Supreme Court nor the First Circuit has addressed whether a border search of electronic devices that store personal information constitutes a non-routine “highly intrusive search” which would require some level of suspicion. However, the Supreme Court has defined those “highly intrusive searches” that do require some level of suspicion and they involve searches of the person. In Montoya de Hernandez, the Supreme Court held that the search of a traveler’s “alimentary canal” was “beyond the scope of a routine customs search and inspection” and that particularized suspicion was required, noting that “[t]he interests in human dignity and privacy which the Fourth Amendment protects forbids any such intrusion [beyond the body’s surface] on the mere chance that desired evidence might be obtained.” 473 U.S. at 540 n. 3 (internal quotation marks and citation omitted). In rejecting that some level of suspicion is required to search vehicles at the border, in Flores-

²The Defendants do not argue that the agents had reasonable suspicion or any reason to conduct the search and seizure but rather rely on the argument that none was required.

Montano, the Supreme Court explained that the “dignity and privacy interests” of “highly intrusive searches of a person” such as strip or body cavity searches “simply do not carry over to vehicles.” 541 U.S. at 152. The First Circuit has noted that the “only types of border search[es] of an individual’s person that have been consistently held to be non-routine are strip-searches and body-cavity searches.” United States v. Braks, 842 F.2d 509, 512-13 (1st Cir. 1988); see Barrow, 448 F.3d at 41 (stating that “[n]on-routine border searches include strip searches and body-cavity searches and can only be made if supported by a reasonable suspicion”); see also United States v. Kallevig, 534 F.2d 411, 414 n. 4 (1st Cir. 1976) (noting that “a border search that is less intrusive than a strip search requires no level of suspicion on the part of customs officials”).

In Braks, in summarizing the analysis of the Supreme Court and several Courts of Appeals, the First Circuit noted that “[t]he degree of invasiveness or intrusiveness associated with any particular type of search determines whether or not that search qualifies as routine,” 842 F.2d at 511, and identified the following factors a court may consider in determining the degree of invasiveness that accompanies any particular search: (1) “whether the search results in the exposure of intimate body parts or requires the suspect to disrobe”; (2) “whether physical contact between Customs officials and the suspect occurs during the search”; (3) “whether force is used to effect the search”; (4) “whether the type of search exposes the suspect to pain or danger”; (5) “the overall manner in which the search is conducted”; and (6) “whether the suspect’s reasonable expectations of privacy, if any, are abrogated by the search.” Id. at 512 (footnotes and citations omitted). The First Circuit explained that the “categorization of a border search as routine or non-routine can[not] be accomplished merely by stacking up and comparing the several factors favoring each of the two classifications” and that the list of factors “is neither intended to be, nor can it be, an exhaustive list

of equally-weighted concerns” because, “[u]ltimately each case must turn upon its own particularized facts.” Id. at 513.³ It is no surprise that the first four factors identified under Braks address physical contact and force, since it is such contact with the person being searched that fundamentally implicates “dignity and privacy interests.” Flores-Montano, 541 U.S. at 152.

Considering these factors in light of Supreme Court precedent, it cannot be said that the search and seizure of House’s laptop and other electronic devices was so intrusive as to require any particularized suspicion. House contends that the search of a laptop and electronic devices implicates one’s “dignity and privacy interests,” not because there was any disrobing, physical search of his person, force used or exposure to pain or danger, but because such devices contain information concerning one’s thoughts, ideas and communications and associations with others. However, such a search of a laptop computer or other electronic devices does not involve the same “dignity and privacy interests” as the “highly intrusive searches of the person” found to require some level of suspicion such as strip searches or body cavity searches. Flores-Montano, 541 U.S. at 152. The Supreme Court has not explicitly held that all property searches are routine or that such searches are categorically incapable of implicating the “dignity and privacy interests of the person being searched,” id., but the search of one’s personal information on a laptop computer, a container that stores

³In Flores-Montano in 2004, the Supreme Court rejected the Ninth Circuit’s approach in fashioning a balancing test to determine whether a border search is “routine” - a test the Ninth Circuit then applied to a vehicle search. 541 U.S. at 152. The Supreme Court stated that “[c]omplex balancing tests [such as this] to determine what is a ‘routine’ search of a vehicle, as opposed to a more ‘intrusive’ search of a person, have no place in border searches of vehicles.” Id. In the absence of subsequent Supreme Court or First Circuit authority overruling the Braks balancing test (articulated by the First Circuit in 1988), this Court has applied it here. Notwithstanding such application, the Court finds that the initial search and seizure search of House’s laptop computer and other electronic devices is nonetheless reasonable under the Fourth Amendment.

information, even personal information, does not invade one's dignity and privacy in the same way as an involuntary x-ray, body cavity or strip search of person's body or the type of search that have been held to be non-routine and require the government to assert some level of suspicion.

Rather, the search of House's laptop and electronic devices is more akin to the search of a suitcase and other closed containers holding personal information travelers carry with them when they cross the border which may be routinely inspected by customs and require no particularized suspicion. The search of a laptop computer at the border is not vastly distinct from "suspicionless border searches of travelers' luggage that the Supreme Court [has] allowed." United States v. Arnold, 533 F.3d 1003, 1009 (9th Cir. 2008). In the Ninth Circuit's decision in Arnold, the court concluded that customs officials did not need reasonable suspicion to search a laptop or other personal electronic storage devices at the border. Id. at 1008. In so concluding, Arnold reasoned that the search of a piece of property like a laptop or other electronic device "does not implicate the same 'dignity and privacy' concerns as a 'highly intrusive search of a person.'" Id. (quoting Flores-Montano, 541 U.S. at 152). In the Fourth Circuit's decision in United States v. Ickes, 393 F.3d 501, 504-506 (4th Cir. 2005), the court rejected the constitutional challenge to a border search of a computer and required no reasonable suspicion to be searched at the border given the government's broad authority under the border search doctrine to search the belongings of all entrants without establishing probable cause or a warrant. Other courts have similarly found that the search of various electronic devices storing a traveler's information may be searched at the border without any particularized suspicion. See United States v. Linarez-Delgado, 259 Fed. Appx. 506, 508 (3d Cir. 2007) (finding that the search of the defendant's videotape when the defendant re-entered the country did not require reasonable suspicion); Cancel-Rios v. United States, 2010 WL 3420805, at *3 (D.P.R. Aug. 30, 2010) (noting

that the search of a traveler's cell phone did not require any particularized suspicion and therefore concluding that it was not deficient performance by the petitioner's counsel for not having pursued a motion to suppress this evidence). The other cases cited by House, Pl. Opp. at 16, do not undermine the soundness of the reasoning in Arnold and Ickes as the courts in those cases either declined to decide whether reasonable suspicion existed for the search, United States v. Irving, 452 F.3d 110, 123-24 (2d Cir. 2006) (involving border search of a person's luggage or personal belongings the Court found to be a categorically routine search), concluded that the government needed no reasonable suspicion to conduct the search and even if reasonable suspicion was required, such suspicion existed for the search, United States v. Hampe, 2007 WL 1192365, at *4 (D. Me. Apr. 18, 2007), report and recommendation adopted by, 2007 WL 1806671 (D. Me. June 19, 2007) (involving a border search of files located on a computer's desktop); United States v. Bunty, 617 F. Supp. 2d 359, 364-65 (E.D. Pa. 2008) (involving a border search of defendant's computer equipment); United States v. Furukawa, 2006 WL 3330726, at *1 (D. Minn. Nov. 16, 2006) (concluding that it "need not determine whether a border search of a laptop is 'routine' for purposes of the Fourth Amendment because, regardless, the magistrate judge correctly found the customs official had a reasonable suspicion in this case"), or assumed the search to be non-routine, but nonetheless affirmed the district court's holding on reasonable suspicion grounds, United States v. Roberts, 274 F.3d 1007, 1012 (5th Cir. 2001).

It is the level of intrusiveness of the search that determines whether the search is routine, not the nature of the device or container to be searched. See, e.g., United States v. Giberson, 527 F.3d 882, 888 (9th Cir. 2008) (stating that "neither the quantity of information, nor the form in which it is stored, is legally relevant in the Fourth Amendment context"). Carving out an exception for

information contained on electronic devices would provide travelers carrying such devices with greater privacy protection than others who choose to carry the same type of personal information in hard copy form.⁴ Id. at 888 (noting that “attempting to limit Fourth Amendment searches based on the format of stored information would be arbitrary”). Such a distinction is arbitrary since it cannot be said that House has any greater expectation of privacy in the information stored on his computer than in personal information he might carry in papers stored in a briefcase at the border. Requiring reasonable suspicion for all computer searches may “allow individuals to render graphic contraband, such as child pornography, largely immune to [a] border search simply by scanning images onto a computer disk before arriving at the border.” United States v. Irving, 2003 WL 22127913, at *5 (S.D.N.Y. Sept. 15, 2003). Thus, the level of suspicion required to conduct a search of information carried by a person should not be based on the form in which that information is kept and presented at the border. For these same reasons, the nature and quality of the information on the electronic devices searched cannot, alone, make the search particularly offensive so as to require a heightened level of suspicion.

House further alleges that he was targeted by customs officials for a search of his electronic devices because of his affiliation with the Manning Support Network. (Compl. ¶ 14). Accepting as

⁴Contrary to House’s contentions, see Pl. Opp. at 14, the search of his laptop and other electronic devices is not akin to the search of one’s home or private cabin on a ship. Neither a private cabin on a ship or a home is a device for storing information that a person carries with them across the border. See Arnold, 533 F.3d at 1009 (stating that “beyond the simple fact that one cannot live in a laptop . . . a laptop goes with the person,” and is thus mobile). As the Supreme Court noted in Ramsey, “a port of entry is not a traveler’s home. His right to be let alone neither prevents the search of his luggage nor the seizure of unprotected, but illegal, materials when his possession of them is discovered during such a search.” 431 U.S. at 618 (quoting United States v. Thirty-Seven Photographs, 402 U.S. 363, 376 (1971)).

true House’s allegations concerning the officials’ subjective motivations for searching his electronic devices, the Court nonetheless may not consider the underlying intent or motivation of the officers when analyzing the viability of a Fourth Amendment claim, *see Whren v. United States*, 517 U.S. 806, 813 (1996) (stating that “we have been unwilling to entertain Fourth Amendment challenges based on the actual motivations of individual officers”); *Irving*, 452 F.3d at 123 (noting that “[a]s pretext should not determine the validity of a border search, it also should not determine whether a border search is routine”), which House appears to acknowledge. (Pl. Sur-reply at 11). The Court declines to do otherwise here at least in regard to House’s Fourth Amendment claim.

B. Fourth Amendment Challenge to the Duration of the Seizure of House’s Devices

House argues that even if this Court rejects its argument that reasonable suspicion was required for the search on November 3, 2010, the Defendants still violated his Fourth Amendment right to be free from unreasonable searches and seizures because of their prolonged detention of his electronic devices for forty-nine days. (Pl. Opp. at 19). The Defendants disagree, arguing that they have the authority to detain electronic devices seized at the border for as long as it takes to adequately inspect those devices. (Def. Mem. at 19-21).

House relies on *United States v. Place*, 462 U.S. 696, 708-710 (1983) to support his argument that the Court here should require reasonable suspicion for the forty-nine-day detention of his electronic devices. There, the Court held that probable cause was the appropriate standard for the ninety-minute detention of luggage and noted that seizing luggage in a person’s immediate possession “intrudes on both the suspect’s possessory interest in his luggage as well as his liberty interest in proceeding with his itinerary.” *Id.* at 708. However, *Place* involved a domestic search and seizure, not one conducted at the international border where an individual’s expectation of privacy

is diminished, Montoya de Hernandez, 473 U.S. at 539 and where the “Government’s interest in preventing the entry of unwanted persons and effects is at its zenith” Flores-Montano, 541 U.S. at 152. Although Place is distinguishable because the initial detention did not occur at the border, the inquiry into the reasonableness of the duration of a seizure is nonetheless an appropriate consideration under the Fourth Amendment analysis. 462 U.S. at 709-10. That is, even if the initial seizure of a laptop and other electronic devices at the border requires no reasonable suspicion, the “[g]overnment cannot simply seize property under its border search power and hold it for weeks, months, or years on a whim.” United States v. Cotterman, 637 F.3d 1068, 1070, 1082-83 (9th Cir. 2011) (finding that a two-day seizure of the defendant’s laptop was reasonable, but only after a full account of what the government was doing with the laptop to ensure that it was acting expeditiously when it had possession of it was produced), reh’g en banc granted, ___ F.3d ___, 2012 WL 931079 (9th Cir. Mar. 19, 2012). The duration of the seizure must be “reasonably related in scope to the circumstances which justified it initially.” Id. at 1082 (extending the Montoya de Hernandez rule to agents’ search of laptops). House alleges it was not.

Accordingly, the Court concludes that House has alleged a plausible basis for this claim in his complaint, but the Court cannot determine, as the Defendants urge it to do, at this stage in the proceedings whether the 49-day detention of House’s electronic devices was reasonably related in scope to the circumstances that may have justified it at the border. The Defendants point out that ICE policy provides that searches of electronic devices are to be completed within thirty calendar days of the date of the detention, unless circumstances exist that warrant more time. (Def. Statement of Facts, ICE Directive No. 7-6.1 at ¶ 8.3(1)). There is no dispute between the parties that the detention of House’s electronic devices exceeded this limit, but the Defendants argue that here, the

inspection of House's electronic devices for more than thirty days was reasonable under the circumstances. Specifically, they argue that because House did not provide his password for the laptop, ICE spent additional time reviewing his devices. (Def. Mem. at 22). The Defendants further argue that ICE agents were not familiar with the software and operating system on House's laptop and as a result, they needed to take additional steps to ensure that the images of plaintiff's devices were made correctly. (Def. Mem. at 22-23). The Defendants also contend that there are a limited number of ICE agents certified in computer forensics, thus requiring more time for those agents to review House's devices. (Def. Mem. at 23).

House disputes the reasonableness of the prolonged seizure of House's electronic devices and has produced a declaration from Alexander Stamos, a forensic investigator, to support House's argument that a forty-nine-day seizure to review and analyze his electronic devices was not a reasonable amount of time. (Pl. Opp., Declaration of Alexander Stamos ("Stamos Decl.")). Stamos attests that the process of imaging and verification described in the Declaration of ICE agent Robert Marten (attached as Exhibit 4 to Def. Statement of Facts) should not have taken more than eighteen hours, did not require the one-week period that the devices were retained by ICE in Chicago and did not require the period of nearly six weeks that the devices were retained in New York. (Stamos Decl. at ¶ 6). The Defendants do not explain the extent to which the limited number of ICE agents certified in computer forensics and their current workload prolonged the detention of House's electronic devices or how the transferring of the devices affected that delay and the factual record remains undeveloped as to these issues material to the reasonableness of the duration of the seizure and House disputes the rationale proffered by the Defendants for the forty-nine-day delay. The Court concludes that House has asserted a plausible Fourth Amendment claim in this respect and it declines

to convert the Defendants' motion and grant summary judgment in their favor at this juncture and on the record currently before the Court. Accordingly, the Defendants' motion to dismiss House's Fourth Amendment Claim is DENIED.

C. First Amendment Challenge to the Search and Seizure

House alleges that the agents' search and prolonged detention of his electronic devices and the retention and dissemination of the data therein violated the First Amendment (Second Cause of Action, Compl. ¶ 37) and "[t]he interception and, more particularly, the retention and dissemination of information in [his] computer and other electronic devices regarding the organization, work, and supporters and donors of the Bradley Manning Support Network violate the right of associational privacy guaranteed by the First Amendment." (Compl. ¶ 38).

1. The Court Declines to Dismiss House's First Amendment Claim

The First Amendment to the United States Constitution provides that "Congress shall make no law . . . abridging the freedom of speech . . . or the right of the people peaceably to assemble." U.S. CONST. amend. I. An individual's First Amendment rights may not be violated simply because a search uncovers expressive material. See Zurcher v. Stanford Daily, 436 U.S. 547, 563-68 (1978) (finding that the execution of search warrant to locate evidence - identifying individuals who attacked police officers in a particular incident - at the office of a student newspaper during which officers searched filing cabinets, desks and had the opportunity to read staffers' notes and correspondence did not violate the Fourth or First Amendments). However, the search in this case is alleged to have targeted specifically House's expressive material concerning the Support Network. The complaint further alleges that the agents stopped him at the border because of his association with Manning and the Support Network. Compl. ¶¶ 14, 19. When agents Santiago and Louck stopped House while

he was en route to his connecting flight, they directed him to surrender the electronic devices he was carrying. Id. at ¶¶ 16-17. They questioned him for an extended period of time only after seizing his devices. Id. at ¶¶ 17, 19. When the agents questioned House, they did not ask him any questions related to border control, customs, trade, immigration, or terrorism and did not suggest that House had broken the law or that his computer may contain illegal material or contraband. Id. at ¶ 19. Rather, their questions focused solely on his association with Manning, his work for the Support Network, whether he had any connections to WikiLeaks, and whether he had contact with anyone from WikiLeaks during his trip to Mexico. Id. Thus, the complaint alleges that House was not randomly stopped at the border; it alleges that he was stopped and questioned solely to examine the contents of his laptop that contained expressive material and investigate his association with the Support Network and Manning.⁵ Although the Defendants' motivation to search and retain House's devices for their material concerning the Support Network and Manning, as alleged in the complaint, is not relevant to the Court's analysis of his Fourth Amendment claim, it is pertinent to House's First Amendment claim. See Bd. of Educ., Island Trees Union Free Sch. Dist. No. 26 v. Pico, 457 U.S. 853, 870-71 (1982) (finding motivation of school board in its decision to remove certain books from the school library relevant in determining whether removal was unconstitutional under the First Amendment).

⁵The complaint alleges that the search and seizure that occurred on November 3, 2010 at the border occurred against a backdrop of federal agencies targeting House's associational activity with the Support Network. House alleges that federal agencies first took an interest in him after his role in the creation of the Support Network and have questioned him in his home and at work about his political activities, beliefs and have monitored his activities. Id. at ¶ 14. House further alleges that his name has been placed on a watch list, which has resulted in the tracking of his travel and in being subjected to detention and to different searches at the border by government agencies. Id.

The Defendants do not suggest that the detention of House's devices was necessary to detect information relating to "terrorism, narcotics smuggling, and other national security matters; alien admissibility; contraband or trademark laws; and evidence of embargo violations or other import or export control laws," Def. Statement of Facts, ICE Directive No. 7-6.1 at ¶ 4, but that only incidentally, the agents stumbled upon information concerning the Support Network which does not implicate House's First Amendment rights. Def. Mem. at 26; Def. Reply at 10-11. The Defendants also suggest that most of the questions the agents posed to House concerned Manning, who was under criminal investigation at the time of the search and seizure, and not the Support Network. Def. Reply at 13 n. 10; 12/20/2011 Hearing Transcript at 17-18.

To support their argument that there is no First Amendment exception to the border search doctrine, the Defendants rely on the Fourth Circuit's decision in Ickes and the Ninth Circuit's decision in Arnold, each declining to carve out a First Amendment exception for the search of electronic devices simply because they contained expressive material. The facts surrounding the seizures in Ickes or Arnold are different in some significant respects than those alleged in the complaint here. In Arnold, although the Court held that customs officers did not need reasonable suspicion to search a laptop or other personal electronic storage devices at the border, the officers at the border examined the visible files on the computer and found what appeared to be child pornography. 533 F.3d at 1005. The officers did not seize the computer for an indefinite period of time until after they identified what seemed to be illegal material. Id. Similarly, in Ickes, the agents did not inspect the contents of the defendant's computer until after they had discovered marijuana paraphernalia, photo albums of child pornography, a disturbing video focused on a young ball boy, and an outstanding warrant for the defendant's arrest. 393 F.3d at 507. In holding that the Defendant had failed to state

a First Amendment claim, the Fourth Circuit noted that “[a]s a practical matter, computer searches are most likely to occur where-as here-the traveler’s conduct or the presence of other items in his possession suggest the need to search further.” Id. In contrast to the searches and seizures at issue in Arnold and Ickes, here, the complaint alleges that the agents targeted House and stopped him at the airport specifically because of his association with the Support Network. Before even questioning House, the agents seized his electronic devices and in seizing them for forty-nine days, reviewed, retained, copied and disseminated information about the Support Network. Although the agents may not need to have any particularized suspicion for the initial search and seizure at the border for the purpose of the Fourth Amendment analysis, it does not necessarily follow that the agents, as is alleged in the complaint, may seize personal electronic devices containing expressive materials, target someone for their political association and seize his electronic devices and review the information pertinent to that association and its members and supporters simply because the initial search occurred at the border. See Roaden v. Kentucky, 413 U.S. 496, 501 (1973) (noting that “[a] seizure reasonable as to one type of material in one setting may be unreasonable in a different setting or with respect to another kind of material”); see also Ramsey, 431 U.S. at 624 (noting that any chill that might exist may be minimal and wholly subjective where customs officers opened envelopes at the border when they had reason to believe they contained something other than correspondence, while the reading of the correspondence inside the envelopes was forbidden).

2. House States a Claim for Violation of his Right to Freedom of Association under the First Amendment

The Supreme Court has “long understood as implicit in the right to engage in activities protected by the First Amendment a corresponding right to associate with others in pursuit of a wide

variety of political, social, economic, educational, religious, and cultural ends.” Roberts v. United States Jaycees, 468 U.S. 609, 622 (1984) (citing cases). That is, “[t]he First Amendment protects political association as well as political expression.” Buckley v. Valeo, 424 U.S. 1, 15 (1976). The right of expressive association “is especially important in preserving political and cultural diversity and in shielding dissident expression from suppression by the majority.” Roberts, 468 U.S. at 622. The government may nonetheless engage in some conduct that “might make it more difficult for individuals to exercise their freedom of association, [but] this consequence does not, without more, result in violation of the First Amendment.” Fighting Finest, Inc. v. Bratton, 95 F.3d 224, 228 (2d Cir. 1996). “To be cognizable, the interference with associational rights must be ‘direct and substantial’ or ‘significant.’” Id. (quoting Lyng v. Int’l Union, 485 U.S. 360, 366, 367 & n. 5 (1988) (further citation omitted)). The complaint alleges, and the Defendants do not dispute, that House has a protected right to express himself through his association with the Support Network. The only question, therefore, is whether the complaint adequately alleges an interference with House’s associational rights that was “direct and substantial” or “significant.” Id.

Here, the complaint’s allegations are sufficient to support a reasonable inference that the agents’ interferences with House’s associational rights were direct and substantial to state a plausible right of association claim. As discussed above, the agents questioned House solely about his association with Manning, his work for the Support Network, whether he had any connections to WikiLeaks, and whether he had contact with anyone from WikiLeaks during his trip to Mexico. Id. at ¶ 19. None of their questions concerned border control, customs, trade, immigration, or terrorism. Id. House alleges he was questioned solely because of his association with the Support Network and

Manning and so that the agents could search the information on his laptop and other electronic devices.

Because of the seizure of his laptop and other devices, House alleges that the Defendants are now in possession of the complete, confidential list of the Support Network members and supporters, as well as email and documents detailing the Support Network's inner workings. Id. at ¶¶ 27, 28, 30, 33. The complaint also alleges that the information was copied and retained by ICE and that it has been disseminated to other government agencies. Id. at ¶ 27. And, as House has alleged, because there are supporters and donors to Manning's defense who wish to remain anonymous, the seizure of House's records by Defendants and the access to that information by other government agencies will deter support for the organization in the future and chill the associational rights of the Support Network and its supporters. Id. at ¶¶ 33, 35, 38. Compulsory disclosure of the Support Network's members, supporters and internal communications of the organization, as that which is alleged here, "can seriously infringe on privacy of association and belief guaranteed by the First Amendment," Buckley, 424 U.S. at 64, and can "have . . . a profound chilling effect" Perry v. Schwarzenegger, 591 F.3d 1126, 1135 (9th Cir. 2009); see also AFL-CIO v. FEC, 333 F.3d 168, 175 (D.C. Cir. 2003) (noting that the "Supreme Court has long recognized that compelled disclosure of political affiliations and activities can impose just as substantial a burden on First Amendment rights as can direct regulation").

The Defendants argue that any infringement on House's right of association was incidental to a valid exercise of the agents' authority to search and detain his items at the border. (Def. Mem. at 26). The Defendants rely on a series of cases to support their argument that House cannot state a First Amendment associational claim because he has failed to show a form of retaliation, harassment

or intimidation by the government, (Def. Mem. at 27), but each case the Government cites concerned whether the evidence was sufficient to support a First Amendment claim at the summary judgment stage. See, e.g., Lyng, 485 U.S. at 367 n.5 (noting that the “facts . . . do not demonstrate any ‘significant’ interference” with appellees’ associational rights); Doyle v. N.Y. State Div. of Hous. and Cmty. Renewal, 1999 WL 177441, at *7-8 (S.D.N.Y. Mar. 30, 1999) (finding evidence presented on summary judgment was insufficient to support First Amendment claim); see also In re Motor Fuel Temperature Sales Practices Litig., 641 F.3d 470, 489 (10th Cir. 2011) (finding that appellants failed to make “an evidentiary showing of a reasonable probability of chill on an association right” sufficient to support granting a writ of mandamus) (internal citation omitted). Moreover, the Supreme Court has noted that “associational rights are protected not only against heavy-handed frontal attack, but also from being stifled by more subtle governmental interference and that these rights can be abridged even by government actions that do not directly restrict individuals’ ability to associate freely.” Lyng, 485 U.S. at 367 n. 5 (internal quotation marks and citation omitted).

At this juncture, House has alleged sufficient facts to support his First Amendment claim and any dispute as to what the evidence will or will not show is best answered at summary judgment or trial on the basis of discovered facts, not at this stage on the pleadings. Cf. Tabbaa v. Chertoff, 509 F.3d 89, 105-106 (2d Cir. 2007) (granting summary judgment in defendants’ favor on First Amendment claim because the government had offered sufficient evidence to establish that it had a compelling interest in preventing suspected terrorists who had attended the conference from entering the United States and that it could not have achieved that interest through means less restrictive of plaintiffs’ associational freedoms).

The Defendants’ assertion that concluding that House has alleged a plausible First Amendment claim would be somehow inconsistent with the Court’s finding that the initial search and seizure was routine under the Fourth Amendment analysis ignores the difference in legal standards that apply to Fourth Amendment and First Amendment claims. See Tabbaa, 509 F.3d at 102 n. 4 (noting that “distinguishing between incidental and substantial burdens under the First Amendment requires a different analysis, applying different legal standards, than distinguishing what is and is not routine in the Fourth Amendment border context”). That the initial search and seizure occurred at the border does not strip House of his First Amendment rights, particularly given the allegations in the complaint that he was targeted specifically because of his association with the Support Network and the search of his laptop resulted in the disclosure of the organizations, members, supporters donors as well as internal organization communications that House alleges will deter further participation in and support of the organization. Accordingly, the Defendants’ motion to dismiss House’s First Amendment claim is DENIED.

D. House’s Request for Injunctive Relief Regarding the Dissemination and Retention of the Information on his Electronic Devices

House seeks, among other forms of relief, an injunction requiring the Defendants to reveal to whom they disclosed or disseminated information contained on his electronic devices, (Compl., Prayer for Relief, C), and an injunction requiring them to return all information obtained from House’s electronic devices and if the information cannot be returned, to expunge or otherwise destroy it. (Compl., Prayer for Relief, B). The Defendants argue that even if House is ultimately successful on his Constitutional claims, he is nonetheless not entitled to this form of injunctive relief. The Court need not reach this issue, as it is premature at this stage in the proceedings. “An injunction is an

exercise of a court's equitable authority, to be ordered only after taking into account all of the circumstances that bear on the need for prospective relief." Salazar v. Buono, ____ U.S. ____, 130 S.Ct. 1803, 1816 (2010). The Supreme Court has instructed courts to be "particularly cautious when contemplating relief that implicates public interests." Id. (and cases cited). The Court proceeds in such manner here particularly in light of the Defendants' argument that granting the type of relief requested here would compromise law enforcement functions ICE performs for the Government as it could inhibit (or interfere with) appropriate information sharing between agencies that would identify threats to the United States. (Def. Reply at 16). Because the Court does not have before it all of the discovered facts as it would at a later stage at summary judgment or trial, the Court is unable to adequately assess all of the circumstances that would bear on the issuance for an injunction in the particular form requested by House at this time.

VI. Conclusion

For the foregoing reasons, the Defendants' motion to dismiss is DENIED.

So ordered.

/s/ Denise J. Casper
United States District Judge